



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

HN

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/068,401	02/06/2002	Sewim F. Ablay	CM04288H	9611
22917	7590	02/02/2006	EXAMINER	
MOTOROLA, INC. 1303 EAST ALGONQUIN ROAD IL01/3RD SCHAUMBURG, IL 60196			HOFFMAN, BRANDON S	
			ART UNIT	PAPER NUMBER
			2136	

DATE MAILED: 02/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)
	10/068,401	ABLAY ET AL.
	Examiner	Art Unit
	Brandon S. Hoffman	2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 29 November 2005.  
 2a) This action is FINAL. 2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-3 and 5-46 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-3 and 5-46 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
 Paper No(s)/Mail Date 10-20-05.

4) Interview Summary (PTO-413)  
 Paper No(s)/Mail Date. \_\_\_\_\_.  
 5) Notice of Informal Patent Application (PTO-152)  
 6) Other: \_\_\_\_\_.

## DETAILED ACTION

1. Claims 1-3 and 5-46 are pending in this office action.
2. Applicant's arguments, filed November 29, 2005, have been fully considered but they are not persuasive.

### ***Claims Rejections***

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

### ***Claim Rejections - 35 USC § 102***

4. Claims 1-3, 5-7, 10-15, 17-22, 25-35, and 37-46 are rejected under 35 U.S.C. 102(e) as being anticipated by Harif (U.S. Patent Pub. No. 2002/0133716).

Regarding claims 1, 17, and 27-29, Harif teaches a method/apparatus for authenticating an entity in a vehicle, the method/apparatus comprising:

---

- A first, trusted entity residing in the vehicle (fig. 1, ref. num 14);
- A second entity residing in the vehicle and in communication with the trusted entity (fig. 1, ref. num 18); and
- Wherein the trusted entity receives a service request, determines whether the second entity is an authenticated entity in response to the service request, and,

when the second entity is not an authenticated entity, authenticates the second entity to produce an authenticated entity **and grants the service request** (fig. 6, ref. num 106 & 108 and paragraph 0049),

- **Wherein the trusted entity is a vehicle gateway** (paragraph 0057, the primary encoding device is a trusted source within the vehicle), **and**
- **Wherein the second entity is one of a wireless gateway, a vehicle system, and a user system** (paragraph 0058, programmable key is used in a vehicle system to perform a variety of tasks).

Regarding claims 2, 18, and 30, Harif teaches wherein the trusted entity stores a list of authenticated entities and determines whether the second entity is an authenticated entity by reference to the list (paragraph 0032, discussion on certificates).

Regarding claims 3, 19, and 31, Harif teaches wherein the trusted entity stores a list of authenticated entities and adds the second entity to the list when the trusted entity authenticates the second entity (paragraph 0038).

---

Regarding claims 5, 20, and 32, Harif teaches wherein the step of authenticating the entity comprises steps of requesting, from the entity, a certificate comprising a vehicle manufacturer signature, receiving a message comprising the requested certificate, and determining whether the entity is an authenticated entity based on the received message (paragraph 0032).

Regarding claims 6, 21, and 37, Harif teaches wherein the message comprising the requested certificate further comprises an entity signature and an entity manufacturer signature (paragraph 0032, the certificate contains a signature from the manufacturer).

Regarding claims 7, 22, 33, and 34, Harif teaches wherein the step of authenticating the entity further comprises steps of verifying at least one of the vehicle manufacturer signature, the entity signature, and the entity manufacturer signature, and wherein the step of determining whether the entity is an authenticated entity comprises a step of determining whether the entity is an authenticated entity based on the verification of at least one of the vehicle manufacturer signature, the entity signature, and the entity manufacturer signature (fig. 6, ref. num 106 and paragraph 0049).

Regarding claim 10, Harif teaches further comprising a step of determining whether to reprogram the entity when the second entity is an authenticated entity (paragraph 0037).

---

Regarding claims 11 and 40, Harif teaches wherein the step of determining whether to reprogram the entity comprises steps of retrieving vehicle system status information from the entity, and determining whether to reprogram the entity based on the retrieved vehicle system status information (paragraph 0037, identification tags).

Regarding claims 12 and 41, Harif teaches further comprising steps of in response to a determination to reprogram the entity, reprogramming the entity with new software, when the entity is reprogrammed, executing the new software by the entity to produce a result, conveying the result to the trusted entity, and determining whether the reprogramming is successful based on the result (paragraph 0037 and fig. 6, repeating the entire authentication process).

Regarding claims 13, 14, 26, and 42, Harif teaches wherein the entity is a vehicle system that comprises vehicle system status information and wherein the method further comprises steps of retrieving vehicle system status information from the entity, transmitting the retrieved vehicle system status information, and receiving new software in response to the transmission of vehicle system status information (paragraph 0037, identification tags and fig. 6, repeating the entire authentication process).

Regarding claims 15 and 43, Harif teaches wherein the vehicle status information comprises at least one of a current date, a current time, a current location of the vehicle, a current mileage of the vehicle, a vehicle identification number, and an engine diagnostic code (paragraph 0016).

---

Regarding claims 25 and 35, Harif teaches further comprising a step of, when the entity is an authenticated entity, granting the request for service (fig. 6, ref. num 108).

Regarding claim 38, Harif teaches wherein when the second entity is an authenticated entity, the trusted entity determines whether to reprogram the entity and, in response to a determination to reprogram the entity, reprograms the second entity with new software (paragraph 0037 and fig. 6, repeating the entire authentication process).

Regarding claim 39, Harif teaches wherein the second entity is a vehicle system that comprises vehicle system information and wherein the trusted entity retrieves vehicle system status information from the vehicle system and determines whether to reprogram the entity based on the vehicle system information (paragraph 0037, identification tags).

Regarding claim 45, Harif teaches wherein a vehicle gateway performs the steps of receiving, determining, authenticating, and granting (paragraph 0057, the primary encoding device is a trusted source within the vehicle).

Regarding claim 46, Harif teaches further comprising the steps of when the entity is an authenticated entity, receiving service requests from the authenticated entity (fig. 6, ref. num 108).

5. Claims 8, 9, 16, 23, 24, 36, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Harif (U.S. Patent Pub. No. 2002/0133716) in view of Menezes et al. ("Handbook of Applied Cryptography," CRC Press LLC, 1997, pps. 397-405 & 493-495).

Regarding claims 8, 23, and 36, Harif teaches all the limitations of claims 1, 17, and 27, respectively, above. However, Harif does not teach authenticating by generating a random number and using a challenge-response protocol.

Menezes et al. teaches wherein the step of authenticating the entity comprises steps of generating a first random number, conveying, to the entity, the first random number and a request that the entity send a certificate comprising a vehicle manufacturer signature, receiving a message comprising the certificate having a vehicle manufacturer signature and further comprising an entity signature, and entity manufacturer signature, the first random number, and a second random number, and wherein the step of determining whether the entity is an authenticated entity comprises a step of determining whether the entity is an authenticated entity based on the verification of at least one of the vehicle manufacturer signature, the entity signature, and the entity manufacturer signature (page 404, section (i)).

---

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine authenticating an entity by a challenge-response protocol, as taught by Menezes, with the method/apparatus of Harif. It would have been

obvious for such modifications because the challenge-response protocol allows an entity to be authenticated, that is, prove they are who they say they are, without disclosing the actual secret that is being proved (see page 397, section 10.3 of Menezes et al.).

Regarding claims 9, 16, 24, and 44, Harif teaches all the limitations of claims 1, 17, and 27, respectively, above. However, Harif does not teach the use of session keys.

Menezes et al. teaches further comprising steps of when the entity is an authenticated entity, generating a session key, and securely conveying the session key to the authenticated entity (page 494, Motivation for use of session keys).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine generating a session key, as taught by Menezes, with the method/apparatus of Harif. It would have been obvious for such modifications because session keys are good in cases where only a short duration of the key use is needed, such as that of updating/reprogramming a programmable key (see page 494 of Menezes et al.).

### ***Response to Arguments***

6. Applicant amends claims 1, 17, and 27.

7. Applicant argues the newly added feature of authenticating "at least one of a wireless gateway, a vehicle system, and a user system" is not taught by Harif (page 11, second paragraph).

Examiner respectfully disagrees. The abstract of Harif says that the authentication is provided for use in a vehicle, buildings, homes, computers, equipment, and intelligence. Paragraph 0057 of Harif shows the primary encoding device (the first trusted entity) is within the vehicle.

### ***Conclusion***

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

*Brandon S. Hoffman*

BH

*Ch*  
Primary Examiner  
Art Unit  
1131  
1131106